CLAIMS

1. A software protection arrangement for protecting software to be run on a wireless device operable for communication over a wireless network, the arrangement including:

identifying means operable to create an identifier which characterises the device on which the protected software is to be run;

authorisation means operable to receive an identifier created by the identifying means to execute a predetermined function on a received identifier to form a derived identifier, execution of the predetermined function being conditional upon verification of a condition required for authorisation of the use of the software;

and the arrangement further comprising enabling means operable to enable execution of the protected software only when in receipt of an enabling identifier from the authorisation means, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the protected software is to be run.

2. The arrangement of claim 1, wherein the enabling means is operable to apply a function to the derived identifier to recover the identifier from which the derived identifier was derived, and to compare the recovered identifier with the identifier created by the identifying means, and to enable or disable execution of the software in accordance with the result of the comparison.

3. The arrangement of claim 1, wherein the protected software is in encrypted form requiring decryption by at least one decryption key for successful execution, the enabling means including decryption means operable to execute a process which includes decryption of the encrypted code, and to use the derived identifier as a key for the process.

4. The arrangement of claim 1, wherein the predetermined function is a function of at least two variables, a received identifier forming one of the variables, and the other variable being a confidential decryption key stored at the authorisation means, and wherein the enabling means is operable to perform a preliminary step to execute a second predetermined function of at least two variables, including the identifier and the derived

identifier, to recover the confidential decryption key for use as a decryption key in decrypting the encrypted code.

5. The arrangement of claim 4, wherein the identifier further includes information characterising the protected software, and the authorisation means is operable to select a confidential decryption key corresponding with the identified software.

6. The arrangement of claim 1, wherein the identifier is derived from information which identifies hardware and/or software present at the device.

7. The arrangement of claim 1, wherein the authorisation means is operable to effect a financial transaction or credit check before allowing execution of the predetermined function.

8. The arrangement of claim 1, wherein the identifying means is operable to create an identifier as aforesaid on each occasion protected software is to run on the device.

9. The arrangement of claim 1, in which the identifying means transmits identifiers to the authorisation means, over the wireless network.

10. The arrangement of claim 9, wherein the authorisation means is operable to transmit derived identifiers to the enabling means by means of the wireless network.

11. The arrangement of claim 1, wherein the enabling means and/or the identifying means are provided by software elements associated with the protected software.

12. An arrangement for use in protecting software to be run on a wireless device operable for communication over a wireless network, the arrangement including:

identifying means operable to create an identifier which characterises the device on which the protected software is to be run;

enabling means operable to receive a derived identifier derived by authorisation means from the identifier created by the identifying means, and the enabling means being further operable to enable execution of the software only when in receipt of an

enabling identifier, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the software is to be run.

13. The arrangement of claim 12, wherein the enabling means are operable to apply a function to the derived identifier to recover the identifier from which the derived identifier was derived, and to compare the recovered identifier with the identifier created by the identifying means, and to enable or disable execution of the software in accordance with the result of the comparison.

14. The arrangement of claim 13, wherein the protected software is in encrypted form requiring decryption by at least one decryption key for successful execution.

15. The arrangement of claim 14, wherein the enabling means include decryption means operable to execute a process which includes decryption of the encrypted code, and to use the derived identifier as a key for the process.

16. The arrangement of claim 12, wherein the derived identifier is derived by a predetermined function which is a function of at least two variables, a received identifier forming one of the variables, and other variable being a confidential decryption key stored at the authorisation means, and wherein the enabling means is operable to perform a preliminary step to execute a second predetermined function of at least two variables, including the identifier and the derived identifier, to recover the confidential decryption key for use as a decryption key in decrypting the encrypted code.

17. The arrangement of claim 16, wherein the identifier further includes information characterising the protected software, whereby the authorisation means may operate to select a confidential decryption key corresponding with the identified software.

18. The arrangement of claim 12, wherein the identifier is derived from information which identifies hardware and/or software present at the device.

19. The arrangement of claim 12, wherein the identifying means is operable to create an identifier as aforesaid on each occasion protected software is to run on the device.

20. The arrangement of claim 12, wherein the enabling means and/or the identifying means are preferably provided by software elements associated with the protected software.

21. An arrangement for use in protection of software to be run on a wireless device operable for communication over a wireless network, the arrangement including:

authorisation means operable to receive an identifier characterising a device on which protected software is to be run, and the authorisation means being operable to execute a predetermined function on a received identifier to form a derived identifier, execution of the predetermined function being conditional upon verification of a condition required for authorisation of the use of the software; and to provide the derived identifier to allow enabling means to enable execution of the software only when in receipt of an enabling identifier which is a derived identifier derived from the identifier of the device on which the software is to be run.

22. The arrangement of claim 21, wherein the predetermined function is a function of at least two variables, a received identifier forming one of the variables, and another variable being a confidential decryption key stored at the authorisation means, wherein a preliminary step is required upon receipt of a derived identifier by enabling means, to execute a second predetermined function of at least two variables, including the identifier and the derived identifier, to recover the confidential decryption key for use as a decryption key in decrypting an encrypted form of the protected software.

23. The arrangement of claim 22, wherein the identifier includes information characterising the protected software, the server being operable to select a confidential decryption key corresponding with the identified software.

24. The arrangement of claim 21, wherein the authorisation means is operable to effect a financial transaction or credit check before allowing execution of the predetermined function.

25. Computer software which, when installed on one or more devices, is operable to provide a software protection arrangement for protecting software to be run on a wireless device operable for communication over a wireless network, the arrangement including:

identifying means operable to create an identifier which characterizes the device on which the protected software is to be run;

authorisation means operable to receive an identifier created by the identifying means to execute a predetermined function on a received identifier to form a derived identifier, execution of the predetermined function being conditional upon verification of a condition required for authorisation of the use of the software;

and the arrangement further comprising enabling means operable to enable execution of the protected software only when in receipt of an enabling identifier from the authorisation means, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the protected software is to be run.

26. Computer software which, when installed on one or more devices, is operable to provide a software protection arrangement including:

identifying means operable to create an identifier which characterizes the device on which the protected software is to be run;

enabling means operable to receive a derived identifier derived by authorisation means from the identifier created by the identifying means, and the enabling means being further operable to enable execution of the software only when in receipt of an enabling identifier, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the software is to be run.

27. A carrier medium for software which, when installed on one or more devices, is operable to provide a software protection arrangement for protecting software to be run on a wireless device operable for communication over a wireless network, the arrangement including:

identifying means operable to create an identifier which characterizes the device on which the protected software is to be run;

authorisation means operable to receive an identifier created by the identifying means to execute a predetermined function on a received identifier to form a derived identifier, execution of the predetermined function being conditional upon verification of a condition required for authorisation of the use of the software;

and the arrangement further comprising enabling means operable to enable execution of the protected software only when in receipt of an enabling identifier from the authorisation means, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the protected software is to be run.

28. The medium of claim 27, the medium being a memory device or a transmission medium on which the software is carried by a propagating signal.

29. A carrier medium for software which, when installed on one or more devices, is operable to provide a software protection arrangement including:

identifying means operable to create an identifier which characterizes the device on which the protected software is to be run;

enabling means operable to receive a derived identifier derived by authorisation means from the identifier created by the identifying means, and the enabling means being further operable to enable execution of the software only when in receipt of an enabling identifier, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the software is to be run.

30. The medium of claim 29, the medium being a memory device or a transmission medium on which the software is carried by a propagating signal.

31. A signal propagating on a transmission medium and carrying software which, when installed on one or more devices, is operable to provide a software protection arrangement for

protecting software to be run on a wireless device operable for communication over a wireless network, the arrangement including:

identifying means operable to create an identifier which characterizes the device on which the protected software is to be run;

authorisation means operable to receive an identifier created by the identifying means to execute a predetermined function on a received identifier to form a derived identifier, execution of the predetermined function being conditional upon verification of a condition required for authorisation of the use of the software;

and the arrangement further comprising enabling means operable to enable execution of the protected software only when in receipt of an enabling identifier from the authorisation means, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the protected software is to be run.

32. A signal propagating on a transmission medium and carrying software which, when installed on one or more devices, is operable to provide a software protection arrangement including:

identifying means operable to create an identifier which characterizes the device on which the protected software is to be run;

enabling means operable to receive a derived identifier derived by authorisation means from the identifier created by the identifying means, and the enabling means being further operable to enable execution of the software only when in receipt of an enabling identifier, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the software is to be run.

33. A signal propagating on a transmission medium and carrying an identifier or derived identifier of a software protection arrangement for protecting software to be run on a wireless device operable for communication over a wireless network, the arrangement including:

identifying means operable to create an identifier which characterizes the device on which the protected software is to be run;

authorisation means operable to receive an identifier created by the identifying means to execute a predetermined function on a received identifier to form a derived identifier, execution of the predetermined function being conditional upon verification of a condition required for authorisation of the use of the software;

and the arrangement further comprising enabling means operable to enable execution of the protected software only when in receipt of an enabling identifier from the authorisation means, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the protected software is to be run.

34. A method of protecting software to be run on a wireless device operable for communication over a wireless network, including the steps of:

creating an identifier which characterizes the device on which the protected software is to be run;

receiving an identifier and executing a predetermined function on a received identifier to form a derived identifier, execution of the predetermined function being conditional upon verification of a condition required for authorisation of the use of the software;

and enabling execution of the protected software only in response to an enabling identifier, the derived identifier serving as an enabling identifier in the event that the derived identifier has been derived by the predetermined function from the identifier of the device on which the protected software is to be run.

35. The method of claim 34, wherein a function is applied to the derived identifier to recover the identifier from which the derived identifier was derived, and to compare the recovered identifier with the identifier created by the identifying means, and to enable or disable execution of the software in accordance with the result of the comparison.

36. The method of claim 34, wherein the protected software is in encrypted form requiring decryption by at least one decryption key for successful execution, the enabling step including a decryption step which includes decryption of the encrypted code, the derived identifier being used as a key for the decryption step.

37. The method of claim 34, wherein the predetermined function is a function of at least two variables, a received identifier forming one of the variables, and the other variable being a confidential decryption key, the enabling step including a preliminary step to execute a second predetermined function of at least two variables, including the identifier and the derived identifier, to recover the confidential decryption key for use as a decryption key in decrypting the encrypted code.

38. The method of claim 34, wherein the identifier is created to include information characterising the protected software, and the confidential decryption key is selected according to the software identified.

39. The method of claim 34, wherein the identifier is derived from information which identifies hardware and/or software present at the device.

40. The method of claim 34, wherein a financial transaction or credit check is effected before allowing execution of the predetermined function.